UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/402,144	09/29/1999	MARTINA HANCK	P991784	5593

29177 7590 06/27/2007

BELL, BOYD & LLOYD, LLP
P.O. BOX 1135
CHICAGO, IL 60690

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
06/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/402,144	HANCK ET AL.	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,10-12,22-33 and 37-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,10-12,22-33 and 37-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on 05/21/07.

2. Claims 1-3, 10-12, 22-33 and 37-48 are pending.

Response to Arguments

3. On pg. 9 of the Remarks, applicant argues that "Kilner proposes a cryptographic function that necessarily relies on flow control of individual data segments (col.1 41-55; col. 2, lines 44-55; col. 3, lines 51-65), as each checksum is specifically directed to changes in specific places of a record database and affiliating an old checksum value from the cumulative checksum (see claim 1)" and hence does not cover the limitations "wherein flow control for the data segments is negated by the commutative operation" in the independent claims. Examiner respectfully disagrees. Applicant's specification discloses that "by using a commutative operation for individual checksums of the data segments, a flow control for the order of the individual data segments is no longer required. Furthermore, it is no longer required to reassemble the complete user data in the original order in which the first commutative checksums were formed. The order of the individual data segments is no longer of significance in the formation of the commutative checksum." (Specification, pg. 4, lines 22-33). In other words, commutative operations enable the first commutative checksum to be validated without reassembling the segments in a certain order. This feature directly applies with the invention of Kilner as follows. The cumulative checksums (A_CRC, V_CRC and

S_CRC) are not dependent on the ordering of the data entries because these are values determined by commutative operations on the individual data CRC checksums; irrespective of the order the data is received and stored into the database, A_CRC, V_CRC and S_CRC values do not change. Hence, contrary to applicant's allegations, Kilner's checksum function does not rely on flow control of individual data segments to validate the checksums.

4. With respect to applicant's argument that Kilner does not disclose performing a commutative operation on segment checksums, because Kilner discloses the checksum as "cumulative checksums" (Remarks, pg. 10, 2nd paragraph), this argument is not sufficient. Merely because Kilner names a type of checksum with a different naming scheme than the terms listed in applicant's claims does not show that the prior art does not meet the limitation. Rather, the functional aspect of the limitation must be compared with the teaching of the prior art. In this case, Kilner explicitly discloses that the checksum uses a commutative technique to generate the cumulative checksum ("Each record checksum is incorporated reversibly into this 32-bit value, by *shifting its CRC-16 left by its record number modulo 16 and XOR-ing it into the cumulative checksum.* This calculation detects the error of an identical record in a different location. An old R_CRC is backed out of the cumulative checksum, by performing the same process with that old R_CRC (i.e. *shift old R-CRC left by its record number and XOR-ing.*)," [emphasis added] col. 3:58-65)

5. Finally, with respect to applicant's argument that there is no motivation to combine the teaching of Kilner and Frezza (Remarks, pg. 11, 2nd full paragraph),

examiner disagrees. Frezza discloses encrypting a checksum using a secret encryption key to prevent access to the checksum by unscrupulous third parties (col. 2:45-66).

6. For the aforementioned reasons, the claims remain rejected under the prior art of record.

Claim Rejections - 35 USC § 103

7. Claims 1-3, 10-12, 22-33 and 37-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kilner USPN 5,649,089 in view of Frezza et al. U.S. Patent No. 4,982,430 (hereinafter Frezza); subject matter in McNamara et al. USPN 4,533,948 is relied upon since the McNamara patent is incorporated by reference into the Frezza patent (hereinafter McNamara).

8. As per claim 10, Kilner discloses an arrangement for forming a first commutative checksum for digital data which are grouped into a number of data segments, the arrangement comprising:

a. an arithmetic and logic unit, (fig. 1, reference nos. 112 and 115)

b. a first segment checksum, which is formed for each of the data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function, (fig. 1, reference no. 124)

c. a commutative operation which forms the first commutative checksum by operating on the segment checksums, wherein flow control for the data segments is negated by the commutative operation (fig. 1, reference no. 130; irrespective of

the order the data is received and stored into the database, A_CRC, V_CRC and S_CRC values remains the same)

9. Kilner does not disclose a cryptographic operation to protect the first commutative checksum. Frezza teaches encrypting integrity values prior to submitting the integrity value over a network link to prevent unauthorized alteration of a message. Frezza, col. 2:45-3:13. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Kilner by including a cryptographic operation to secure the first commutative checksum. One would be motivated to do so to prevent an unscrupulous third party from an unauthorized modification of a transmitted message (Frezza, col. 2:20-25). The aforementioned cover the limitations of claim 10.

10. As per claim 12, the rejection of claim 10 under 35 USC 103(a) as being unpatentable over Kilner in view of Frezza is incorporated herein. In addition, the arrangement also includes the following:

d. an inverse cryptographic operation to form a first commutative checksum from the cryptographic commutative checksum, (Frezza, col. 1:12-19; 5:50-58; McNamara, 7:34-42; 8:25-35; data encrypted by DES has an inverse operation to retrieve the original data; furthermore, every ciphertext is associated with a specific plaintext);

e. a second segment checksum which is formed for each of the data segment of the digital data to which the first commutative checksum is allocated,

a commutative operation which operates on the second segment checksum which forms a second commutative checksum wherein flow control for the data segments is negated by the commutative operation, and a comparator which checks for a match between the second commutative checksum and a reconstructed first commutative checksum, wherein the first and second segment checksum are formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function. (Kilner, 5:5:48-6:15; fig. 3, reference nos. 311 and 312; resync operation regenerates S_CRC; S_CRC is compared with V_CRC. Because the first commutative checksum uses first segment checksums for each data segment using a CRC technique, the second commutative checksum, which is used to verify the validity of the first commutative checksum, also generates second segment checksums for each data segment using a CRC technique).

11. It would be obvious to one of ordinary skill in the art at the time the invention was made to implement a cryptographic operation to secure the first commutative checksum. One would be motivated to do so to prevent an unscrupulous third party from an unauthorized modification of a transmitted message (Frezza, col. 2:20-25). The aforementioned cover the limitations of claim 12.

12. As per claim 11, it is a claim corresponding to claim 12, and it does not teach or define above the information claimed in claim 12. Therefore, claim 11 is rejected as

being unpatentable over Kilner in view of Frezza for the same reasons set forth in the rejection of claim 12.

13. As per claim 37, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10 rejection 35 U.S.C. 103(a). In addition, the cryptographic operations described use a symmetric key methodology (Frezza, col. 1:12-19; 5:50-58; McNamara, 7:34-42; 8:25-35).

14. As per claims 38 and 39, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, the cryptographic operations described use a symmetric key methodology (Frezza, col. 1:12-19; 5:50-58; McNamara, 7:34-42; 8:25-35). The aforementioned cover the limitations of claims 38 and 39.

15. As per claims 40, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for

forming and checking a first commutative checksum as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). In addition, Kilner teaches the commutative operation to establish column parity, which forms the commutative checksums, is an XOR operation (Kilner, col. 3:52-65): the XOR operation exhibits both commutative and associative properties. The aforementioned cover the limitation of claim 40.

16. As per claims 41 and 42, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, Kilner teaches the commutative operation to establish column parity, which forms the commutative checksums, is an XOR operation (Kilner, col. 3:52-65): the XOR operation exhibits both commutative and associative properties. The aforementioned cover the limitations of claims 41 and 42.

17. As per claim 43, Kilner in view of Frezza cover an arrangement as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). Kilner does not expressly disclose archiving the digital data and the cryptographic commutative checksum. However, archiving the elements of a transmission is a standard feature to verify the contents of a transmission to an auditor. The examiner takes Official Notice that archiving transmission elements are standard means to record the transmission to prove the contents and status of the transmission at a latter date (i.e. auditing a transmission). It

would be obvious to one of ordinary skill in the art at the time the invention was made to archive the digital data and the checksum since it preserves a receipt of the transmission. The aforementioned cover the limitations of claim 43.

18. As per claims 44 and 45, Kilner in view of Frezza cover an arrangement as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). Kilner does not expressly disclose archiving the digital data and the cryptographic commutative checksum. However, archiving the elements of a transmission is a standard feature to verify the contents of a transmission to an auditor. The examiner takes Official Notice that archiving transmission elements are standard means to record the transmission to prove the contents and status of the transmission at a latter date (i.e. auditing a transmission). It would be obvious to one of ordinary skill in the art at the time the invention was made to archive the digital data and the checksum since it preserves a receipt of the transmission. The aforementioned cover the limitations of claims 44 and 45.

19. As per claim 46, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10 rejections under 35 U.S.C. 103(a). In addition, as mentioned previously, the digital data is cryptographically protected, and by convention, the cryptographic operation would be

implemented by an ALU. Furthermore, since Kilner discloses sending the digital data as well as the checksum values and commutative checksum value from the active database to a standby database over a network link (col. 3:14-19, and figs.1-4), and Frezza teaches securing the integrity value being transmitting over a digital network, the digital data would necessarily be processed in accordance with a network management protocol. The aforementioned cover the limitation of claim 46.

20. As per claims 47 and 48, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, as mentioned previously, the digital data is cryptographically protected, and by convention, the cryptographic operation would be implemented by an ALU. Furthermore, since Kilner discloses sending the digital data as well as the checksum values and commutative checksum value from the active database to a standby database over a network link (col. 3:14-19, and figs.1-4), and Frezza teaches securing the integrity value being transmitting over a digital network, the digital data would necessarily be processed in accordance with a network management protocol. The aforementioned cover the limitations of claims 47 and 48.

21. As per claims 1-3 and 22-33, they are method claims corresponding to the subject matter covered in the rejections of claims 10-12 and 37-48, and they do not teach or define above the information covered in the rejections of claims 10-12 and 37-48. Therefore, claims 1-3 and 22-33 are rejected under Kilner in view of Frezza for the same reasons set forth in the rejections of claims 10-12 and 37-48.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung Kim
Examiner
AU 2132
June 21, 2007

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER